Aus der Zahlentheorie der quadratischen Formen

Kneser, Martin

Veröffentlicht in:
Abhandlungen der Braunschweigischen Wissenschaftlichen Gesellschaft Band 33, 1982, S.13-17

Verlag Erich Goltze KG, Göttingen

Aus der Zahlentheorie der quadratischen Formen

Von **Martin Kneser**, Göttingen

Herr Präsident, meine Damen und Herren!

Ich möchte mich zunächst ganz herzlich für die große Ehre bedanken, die mir durch die Verleihung der Carl-Friedrich-Gauß-Medaille zuteil geworden ist. Wenn ich diesen Dank traditionsgemäß mit einem Vortrag aus meinem Arbeitsgebiet verbinde, so freue ich mich einerseits natürlich über die Gelegenheit, einmal auch zu Nichtmathematikern über meine Wissenschaft sprechen zu können; andererseits haben wir Mathematiker es dabei nicht ganz leicht, weil viele der heute interessanten Probleme zu ihrer Erklärung einen Begriffsapparat benötigen, den ich hier nicht voraussetzen kann. Ich will daher versuchen, Ihnen auf einem Streifzug durch die Geschichte der Zahlentheorie einige ihrer Fragestellungen nahezubringen. Dies scheint mir schon deshalb gerechtfertigt, weil manche unserer heutigen Probleme ihre Wurzel in dieser langen und interessanten Geschichte haben. Die Mathematiker unter Ihnen muß ich um Nachsicht bitten, wenn ich auf diese Weise viel Altbekanntes erzähle.

Lassen Sie mich mit einer Zahlenspielerei beginnen. Wenn ich „Spielerei" sage, so ist das in keiner Weise abschätzig gemeint. Im Gegenteil, solche Experimente standen am Anfang der Zahlentheorie, und noch heute werden zahlentheoretische Vermutungen auf ähnliche Weise gefunden und in einer großen Zahl von Fällen – zum Teil mit Hilfe von Computern – numerisch nachgeprüft. Einige der interessantesten haben bisher allen Beweisversuchen getrotzt.

$$
\begin{aligned}
1 &= 1^2\\
2 &= 1^2+1^2\\
3 &= 1^2+1^2+1^2\\
4 &= 2^2 = 1^2+1^2+1^2+1^2\\
5 &= 2^2+1^2\\
6 &= 2^2+1^2+1^2\\
7 &= 2^2+1^2+1^2+1^2\\
8 &= 2^2+2^2\\
9 &= 3^2 = 2^2+2^2+1^2\\
10 &= 3^2+1^2 = 2^2+2^2+1^2+1^2\\
11 &= 3^2+1^2+1^2\\
12 &= 3^2+1^2+1^2+1^2 = 2^2+2^2+2^2\\
13 &= 3^2+2^2 = 2^2+2^2+2^2+1^2\\
14 &= 3^2+2^2+1^2\\
15 &= 3^2+2^2+1^2+1^2\\
16 &= 4^2 = 2^2+2^2+2^2+2^2
\end{aligned}
$$

Ich habe Ihnen in einer Tabelle die Zahlen von 1 bis 16 aufgeschrieben und sie in Summanden zerlegt, die Quadratzahlen sind. Dabei habe ich allerdings nicht alle möglichen Zerlegungen berücksichtigt. Zum Beispiel habe ich nicht hingeschrieben, daß die 7 sich als Summe von sieben Einsen schreiben läßt – das wäre langweilig – sondern mich auf diejenigen Zerlegungen beschränkt, die höchstens vier Summanden benötigen. Es zeigt sich, auch bei Vergrößerung der Tabelle, daß man stets mit vier Quadraten auskommt, daß es aber Zahlen gibt, z.B. 7 und 15, bei denen drei nicht reichen. Daß das allgemein bei allen Zahlen so ist, die bei Division durch 8 den Rest 7 lassen, kann man leicht einsehen, wenn man bedenkt, daß bei Division durch 8 jede ungerade Quadratzahl den Rest 1, jede gerade den Rest 0 oder 4 läßt.

Damit haben wir schon empirisch einen wesentlichen Teil der folgenden beiden Sätze gefunden.

Vier-Quadrate-Satz *(Fermat, Euler, Lagrange):*
Jede natürliche Zahl ist Summe von (höchstens) vier Quadratzahlen.

Drei-Quadrat-Satz *(Fermat, Legendre, Gauß):*
Alle natürlichen Zahlen der Formen $8m+1$, $8m+2$, $8m+3$, $8m+5$, $8m+6$ sind Summen von drei Quadratzahlen, jedoch keine der Form $8m+7$.
Eine Zahl $4m$ ist genau dann Summe dreier Quadratzahlen, wenn m es ist.

Der Vier-Quadrate-Satz wurde bereits in der ersten Hälfte des 17. Jahrhunderts von dem großen französischen Mathematiker Pierre Fermat ausgesprochen. Fermat war Jurist und hat für diesen wie für viele andere zahlentheoretische Entdeckungen keinen Beweis hinterlassen. Nach dem, was wir aus seinen Briefen wissen, können wir aber mit Sicherheit annehmen, daß er einen besessen hat. Wie schwierig diese Frage damals war, sehen Sie daran, daß es über hundert Jahre gedauert hat, bis Lagrange nach Vorarbeiten von Euler den ersten überlieferten Beweis veröffentlichte. Heute kann der Satz in einer einführenden Vorlesung über Zahlentheorie hergeleitet werden.

Etwas schwieriger ist der Drei-Quadrate-Satz, für den erst Gauß in seinen Disquisitiones Arithmeticae einen vollständigen Beweis erbracht hat. Gauß gibt dort nicht nur die Lösbarkeitsbedingungen für die Gleichung $n = x_1^2 + x_2^2 + x_3^2$, sondern bestimmt auch gleich die Lösungsanzahl. Wir wollen uns aber lieber der entsprechenden Frage bei vier Quadraten zuwenden, die noch zu Gauß' Lebzeiten von Jacobi beantwortet wurde.

Anzahlsatz *(Jacobi): Mit*
$a_4(n)$ = *Anzahl der Darstellungen* $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$,
$d(n)$ = *Summe aller ungeraden Teiler von n, wird*

$$a_4(n) = \begin{cases} 8d(n) & \textit{wenn n ungerade} \\ 24d(n) & \textit{wenn n gerade} \end{cases} \quad \textit{ist.}$$

Dabei hat man, um die Antwort in so einfacher Gestalt zu bekommen, für $x_1, \ldots, x_4$

auch 0 und negative ganze Zahlen zuzulassen und muß Darstellungen, die sich nur durch die Reihenfolge der x_i unterscheiden, als verschieden zählen.

Dieser Satz ist in zweierlei Hinsicht bemerkenswert. Einmal stellt er eine Beziehung zwischen zwei grundverschiedenen Anzahlen her. Die linke Seite $a_4(n)$ bezeichnet die Anzahl der **additiven** Zerlegungen der Zahl n in Quadrate, während auf der rechten Seite die Summe der Teiler mit der **multiplikativen** Struktur von n zusammenhängt. Zweitens wendet Jacobi zum Beweis eine Methode an, die seitdem viele schöne zahlentheoretische Erkenntnisse hervorgebracht hat. Er untersucht den Ausdruck

$$(1 + 2x + 2x^4 + 2x^9 + 2x^{16} + \ldots)^4 =$$
$$(\sum_{n=-\infty}^{\infty} x^{n^2})^4 = 1 + a_4(1)x + a_4(2)x^2 + a_4(3)x^3 + \ldots$$

in Abhängigkeit von x mit Hilfsmitteln der Funktionentheorie und leitet daraus Aussagen über die Koeffizienten $a_4(n)$ her. Er selber hat übrigens später einen anderen Beweis gegeben, der diese Hilfsmittel vermeidet.

Wir machen jetzt einen Sprung in die Jahre 1881/82. Damals hatte die Pariser Akademie als Preisaufgabe gestellt, die Zerlegung von Zahlen in fünf Quadrate zu behandeln, ähnlich wie Gauß und Jacobi dies für drei und vier getan hatten. Es gingen drei Bearbeitungen ein. Eine wurde als unzureichend abgelehnt, die zwei anderen aber für so bedeutend befunden, daß sie beide mit einem Preis ausgezeichnet wurden. Die eine stammte von dem englischen Mathematiker Henry John Stephan Smith, der das Problem tatsächlich schon mehr als zehn Jahre zuvor wenigstens ansatzweise behandelt hatte – was dem Pariser Preiskomitee entgangen war –, die andere von dem damals noch nicht achtzehnjährigen Königsberger Studenten Hermann Minkowski; sie bildete den Anfang einer Reihe grundlegender Arbeiten über die Zahlentheorie der quadratischen Formen. Diese Arbeiten wurden über fünfzig Jahre später von dem kürzlich in Göttingen verstorbenen Mathematiker Carl Ludwig Siegel wieder aufgenommen und zu einem allgemeinen Theorem geformt, das alle in diesem Vortrag bisher erwähnten Ergebnisse als Spezialfälle enthält. Ich kann Ihnen diesen Satz von Minkowski und Siegel hier nicht formulieren, will ihn aber an zwei einfachen Beispielen erläutern.

Betrachten wir erstens den Ausdruck

$$q = x_1^2 + 4x_2^2 + 4x_3^2 + 4x_4^2$$

also eine Summe von vier Quadratzahlen, von denen mindestens drei gerade sind. Bezeichnen wir mit a(q,n) die Anzahl der Lösungen der Gleichung $q = n$, so besagt der Satz, daß mit der schon bei Jacobi auftretenden Teilersumme d(n)

$$a(q,n) = \left\{\begin{array}{ll} 2d(n) & \text{wenn } n = 4m+1 \\ 0 & \text{wenn } n = 4m+2 \text{ oder } 4m+3 \end{array}\right\}$$

ist (die durch 4 teilbaren Zahlen habe ich der Einfachheit halber weggelassen).

Als zweites Beispiel wählen wir

$$q_1 = x_1^2 + x_2^2 + x_3^2 + 9x_4^2,$$

also Summen von vier Quadratzahlen, von denen mindestens eine durch 3 teilbar ist. Hier würde man eine ähnliche Formel wie im ersten Beispiel vermuten, nur daß wegen des Faktors $9 = 3^2$ die darzustellenden Zahlen nach ihrem Rest bei der Division durch 3 statt durch 4 zu unterscheiden wären. Einige weitere Überlegungen ließen

$$a(q_1,n) = \left\{ \begin{array}{ll} \frac{1}{4}\, a_4(n) & \text{wenn } n = 3m+1 \\ \frac{1}{2}\, a_4(n) & \text{wenn } n = 3m+2 \end{array} \right\}$$

erwarten, was aber leider nicht zutrifft, denn die Zahl $n = 7$ läßt sich nicht in der Form q_1 darstellen, während $a_4(7) = 64$ ist. Der Siegelsche Satz sagt nun in diesem Fall, daß man außer q_1 noch die andere quadratische Form

$$q_2 = 2x_1^2 + 2x_2^2 + 2x_3^2 + 3x_4^2 + 2x_1x_2 + 2x_2x_3 + 2x_3x_4$$

betrachten muß und dann die „gemittelte Darstellungsanzahl" $\frac{1}{3}\, a(q_1,n) + \frac{2}{3}\, a(q_2,n)$ von n durch q_1 und q_2 gleich dem oben fälschlich für $a(q_1,n)$ hingeschriebenen Ausdruck wird.

Diese beiden Beispiele sind nur die allereinfachsten ihrer Art und hätten auch schon mit den Methoden von Jacobi behandelt werden können. Im allgemeinen werden quadratische Formen nicht nur in 3 oder 4, sondern in einer beliebigen Anzahl von Variablen betrachtet, und auf der rechten Seite der Formel treten anstelle von $d(n)$ andere zahlentheoretische Funktionen auf.

Das Theorem von Minkowski und Siegel stellt zweifellos einen Höhepunkt in der Theorie der quadratischen Formen dar. Trotzdem beantwortet es nicht eine der naheliegenden Fragen. Schauen wir uns nochmal das zweite Beispiel mit der Form q_1 an. In diesem Fall ist es nicht schwer, direkt nachzuweisen, daß $n = 7$ die einzige Ausnahmezahl ist, die sich nicht in der Form q_1 darstellen läßt. Aus dem Siegelschen Satz allein läßt sich das aber nicht ablesen. Man hat sich mit solchen Fragen nach dem Verhalten einer einzelnen Form q_1, nicht gekoppelt mit anderen Formen wie oben q_2, schon lange beschäftigt und bereits vor Siegel weitgehende Aussagen machen können. Als Preis, den man für die Unterscheidung zwischen q_1 und der „Verwandten" q_2 zu zahlen hat, bekommt man für die einzelne Darstellungsanzahl $a(q_1,n)$ keine genaue Formel, sondern nur eine Abschätzung, aus der man aber unter günstigen Umständen ablesen kann, daß q_1 alle natürlichen Zahlen (oder alle mit einigen genau angebbaren Ausnahmen) darstellt.

Diese Ergebnisse, die überwiegend mit funktionentheoretischen Hilfsmitteln erzielt werden, will ich Ihnen nicht mehr vorführen, obwohl ich mich selber mit arithmetischen Methoden um solche Probleme bemüht habe, sondern Ihnen zum Abschluß nur noch zwei Beispiele dazu geben.

Das erste Beispiel sei

$$n = x_1^2 + 3x_2^2 + 5x_3^2 + 7x_2^2.$$

Man probiert aus, daß die Gleichung für $n = 2,22$ nicht lösbar ist, findet dann aber lange keine weiteren Ausnahmen und vermutet, daß es keine mehr gibt. Die erwähnten Sätze zeigen, daß es außer 2 und 22 höchstens noch endlich viele natürliche Zahlen n gibt, die sich nicht so darstellen lassen. Im Prinzip geben sie auch Schranken, bis zu denen man nach Ausnahmen suchen müßte, doch scheint die explizite Durchführung nicht ganz einfach zu sein. Dieses Problem gehört sicher nicht zu den grundlegenden Fragen aus der Zahlentheorie der quadratischen Formen, doch ist es bemerkenswert, daß schon bei so einfachen Zahlenbeispielen Schwierigkeiten der numerischen Rechnung auftreten können.

Anders liegt es bei dem zweiten Beispiel

$$n = x_1^2 + x_2^2 + 10x_2^2,$$

das schon 1917 bei dem indischen Mathematiker Ramanujan auftaucht. Er weiß genau, welche geraden Zahlen n dargestellt werden können und kennt die ersten 16 der folgenden 18 ungeraden Ausnahmezahlen:

3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719.

Man weiß bis heute nicht, ob dies alle sind, ja noch nicht einmal, ob es nur endlich viele ungerade Ausnahmezahlen gibt. Dieses Problem als Spezialfall des Verhaltens quadratischer Formen in drei Variablen scheint sehr viel schwerer, aber auch sehr viel interessanter als das vorige.